The Complexity of Algebraic Algorithms for LWE

Matthias Johann Steiner

Alpen-Adria-Universität Klagenfurt, Klagenfurt am Wörthersee, Austria

May 27, 2024

M. Steiner has been supported in part by the European Research Council

(ERC Grant No. 725042)

Outline

Motivation

Learning With Errors (LWE)

- $q, n \in \mathbb{Z}_{\geq 1}$, q a prime.
- χ probability distribution on $\mathbb{Z}$.
- $\boldsymbol{s} \in \mathbb{F}_q^n$ secret vector.
- LWE sample $(\boldsymbol{a}, b) \in \mathbb{F}_q^n \times \mathbb{F}_q$

$$b = \langle \boldsymbol{s}, \boldsymbol{a} \rangle + e = \sum_{i=1}^{n} s_i \cdot a_i + e \in \mathbb{F}_q^n,$$

where $e \leftarrow \chi$.

UNIVERSITÄT KLAGENFURT

erc European Research Council

Motivation

- Typically χ is discrete Gaussian distribution.
  - For simplicity Gaussian heuristic $\chi = \mathcal{N}(0, \sigma)$.

Motivation

- Typically χ is discrete Gaussian distribution.
  - For simplicity Gaussian heuristic $\chi = \mathcal{N}(0, \sigma)$.
- Arora-Ge polynomial model [AG11].
  - Choose interval $[-N, N] \subset \mathbb{Z}$ and set up the polynomial

$$f = x \cdot \prod_{i=1}^{N} (x - i) \cdot (x + i).$$

UNIVERSITÄT KLAGENFURT

erc European Research Council

Motivation

- Typically χ is discrete Gaussian distribution.
  - For simplicity Gaussian heuristic $\chi = \mathcal{N}(0, \sigma)$.
- Arora-Ge polynomial model [AG11].
  - Choose interval $[-N, N] \subset \mathbb{Z}$ and set up the polynomial

$$f = x \cdot \prod_{i=1}^{N} (x - i) \cdot (x + i).$$

  - For LWE sample $(\boldsymbol{a}, b = \langle \boldsymbol{s}, \boldsymbol{a} \rangle + e)$, the polynomial

$$f\left(b - \langle \boldsymbol{x}, \boldsymbol{a} \rangle\right) = 0 \in \mathbb{F}_q[x_1, \ldots, x_n] = \mathbb{F}_q[\boldsymbol{x}]$$

    has root $\boldsymbol{s}$ with probability, $N = t \cdot \sigma$,

$$1 - \mathbb{P}\left[|e| > t \cdot \sigma\right] \geq 1 - \frac{2}{t \cdot \sqrt{2 \cdot \pi}} \cdot \exp\left(-\frac{t^2}{2}\right).$$

Motivation

- LWE polynomial system, $m \geq n$,

$$\mathcal{F}_{\mathrm{LWE}} \colon f\left(b_1 - \langle \boldsymbol{x}, \boldsymbol{a}_1 \rangle\right) = \ldots = f\left(b_m - \langle \boldsymbol{x}, \boldsymbol{a}_m \rangle\right) = 0.$$

- Previous secret recovery via
  - Linearization [AG11].
  - Gröbner bases under semi-regularity assumption [ACF+15].
  - Linearization under semi-regularity assumption [STA20].

Motivation

- LWE polynomial system, $m \geq n$,

$$\mathcal{F}_{\text{LWE}} \colon f\left(b_1 - \langle \boldsymbol{x}, \boldsymbol{a}_1 \rangle\right) = \ldots = f\left(b_m - \langle \boldsymbol{x}, \boldsymbol{a}_m \rangle\right) = 0.$$

- Previous secret recovery via
  - Linearization [AG11].
  - Gröbner bases under semi-regularity assumption [ACF$^+$15].
  - Linearization under semi-regularity assumption [STA20].
- **This work:**
  - Proven Gröbner basis complexity estimation.
  - Framework for worst-case (designer's perspective) Gröbner basis complexity estimation.
  - Incorporating hints into LWE polynomial systems.

DRL Gröbner Basis

$P = K[x_1, \dots, x_n]$, $m = \prod_{i=1}^{n} x_i^{d_i}$, $\boldsymbol{d} = (d_1, \dots, d_n)$

Degree Reverse Lexicographic (DRL) Term Order

$\boldsymbol{a} >_{DRL} \boldsymbol{b}$ if

- $\sum_{i=1}^{n} a_i > \sum_{i=1}^{n} b_i$, or
- $\sum_{i=1}^{n} a_i = \sum_{i=1}^{n} b_i$ and the last non-zero entry of $\boldsymbol{a} - \boldsymbol{b}$ is negative.

DRL Gröbner Basis

$P = K[x_1, \ldots, x_n]$, $m = \prod_{i=1}^{n} x_i^{d_i}$, $\mathbf{d} = (d_1, \ldots, d_n)$

Degree Reverse Lexicographic (DRL) Term Order

$\mathbf{a} >_{DRL} \mathbf{b}$ if

- $\sum_{i=1}^{n} a_i > \sum_{i=1}^{n} b_i$, or
- $\sum_{i=1}^{n} a_i = \sum_{i=1}^{n} b_i$ and the last non-zero entry of $\mathbf{a} - \mathbf{b}$ is negative.

$I = (f_1, \ldots, f_m) \subset P$ ideal, $I = \{ f \mid f = \sum_{i=1}^{m} h_i \cdot f_i,\ h_i \in P \}$

DRL Gröbner Basis [Buc65]

- $I \subset P$ ideal.
- $\mathcal{G} \subset I$ finite basis.
- $(\mathrm{LM}_{DRL}(f) \mid f \in I) = (\mathrm{LM}_{DRL}(g) \mid g \in \mathcal{G})$.

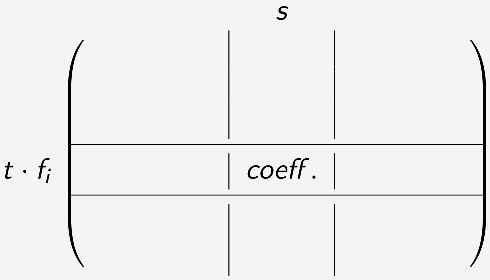
$\mathcal{F} = \{f_1, \ldots, f_m\} \subset P = K[x_1, \ldots, x_n]$

Macaulay Matrix $M_{\leq d}$

- $d \in \mathbb{Z}_{\geq 0}$:

Monomials: $s \in P, \ \deg(s) \leq d$

Polynomials:
$t \in P, \ f_i \in \mathcal{F}$,
$\deg(t \cdot f_i) \leq d$



- Columns sorted via DRL.

Solving Degree

$\mathcal{F} = \{f_1, \ldots, f_m\} \subset P = K[x_1, \ldots, x_n]$

Solving Degree [CG21, Definition 6]

- $\text{sd}_{DRL}(\mathcal{F})$ least $d \in \mathbb{Z}_{\geq 0}$ such that Gaussian elimination on $M_{\leq d}$ produces Gröbner basis.
- Complexity estimate [Sto00]

$$\mathcal{O}\left(m \cdot \text{sd}_{DRL}(\mathcal{F}) \cdot \binom{n + \text{sd}_{DRL}(\mathcal{F}) - 1}{\text{sd}_{DRL}(\mathcal{F})}^{\omega} \right),$$

where $2 \leq \omega \leq 3$.

Degree of Regularity

$\mathcal{F} = \{f_1, \ldots, f_m\} \subset P = K[x_1, \ldots, x_n]$

Degree of Regularity [BFS04, Definition 4]

- $f^{\text{top}} = f^{\text{hom}} \mod (x_0)$.
- $d_{\text{reg}}(\mathcal{F}) = \min\{d \geq 0 \mid (\mathcal{F}^{\text{top}})_d = P_d\}$.
- Heuristic: The larger $|\mathcal{F}|$ the lower $d_{\text{reg}}(\mathcal{F})$.

Degree of Regularity

$\mathcal{F} = \{f_1, \ldots, f_m\} \subset P = K[x_1, \ldots, x_n]$

Degree of Regularity [BFS04, Definition 4]

- $f^{\text{top}} = f^{\text{hom}} \mod (x_0)$.
- $d_{\text{reg}}(\mathcal{F}) = \min\left\{d \geq 0 \mid (\mathcal{F}^{\text{top}})_d = P_d\right\}$.
- Heuristic: The larger $|\mathcal{F}|$ the lower $d_{\text{reg}}(\mathcal{F})$.

$m \geq n + 1$, $d_1 = \deg(f_1) \geq \ldots \geq d_m = \deg(f_m)$

Solving Degree Bound [CG21, Theorem 10, Corollary 2], [Ste24, Theorem 3.2]

- If $d_{\text{reg}}(\mathcal{F}) < \infty$, then
- $\text{sd}_{DRL}(\mathcal{F}) \leq \text{reg}\left(\mathcal{F}^{\text{hom}}\right) \leq \sum_{i=1}^{n+1}(d_i - 1) + 1$.

UNIVERSITÄT KLAGENFURT

erc European Research Council

Proven Complexity for LWE Polynomial Systems

- LWE sample vector matrix: $\operatorname{rank}\begin{pmatrix}\boldsymbol{a}_1 & \dots & \boldsymbol{a}_m\end{pmatrix} = n \Rightarrow d_{\text{reg}}\left(\mathcal{F}_{\text{LWE}}\right) < \infty$.

- LWE sample vector matrix: $\operatorname{rank}\begin{pmatrix}\boldsymbol{a}_1 & \dots & \boldsymbol{a}_m\end{pmatrix} = n \Rightarrow d_{\text{reg}}\left(\mathcal{F}_{\text{LWE}}\right) < \infty$.
- General LWE $q, n, \sigma = \sqrt{\frac{n}{2\cdot\pi}}$

$$\mathcal{O}\left(n \cdot 2^{\omega\cdot\mathcal{O}\left(n^{1.2787}\right)}\right), \quad p_{success} \geq 1 - \frac{2}{\pi \cdot \sqrt{n}}.$$

Proven Complexity for LWE Polynomial Systems

- LWE sample vector matrix: $\operatorname{rank}\begin{pmatrix}\boldsymbol{a}_1 & \dots & \boldsymbol{a}_m\end{pmatrix} = n \Rightarrow d_{\text{reg}}\left(\mathcal{F}_{\text{LWE}}\right) < \infty$.
- General LWE $q, n, \sigma = \sqrt{\frac{n}{2 \cdot \pi}}$

$$\mathcal{O}\left(n \cdot 2^{\omega \cdot \mathcal{O}\left(n^{1.2787}\right)}\right), \quad p_{success} \geq 1 - \frac{2}{\pi \cdot \sqrt{n}}.$$

- Small error LWE $|\mathcal{E}| = D$

$$\mathcal{O}\left(m \cdot (D - 1) \cdot n \cdot 2^{\omega \cdot \mathcal{O}(n)}\right).$$

UNIVERSITÄT KLAGENFURT

erc European Research Council

Proven Complexity for LWE Polynomial Systems

- LWE sample vector matrix: $\operatorname{rank}\begin{pmatrix}\boldsymbol{a}_1 & \dots & \boldsymbol{a}_m\end{pmatrix} = n \Rightarrow d_{\text{reg}}\left(\mathcal{F}_{\text{LWE}}\right) < \infty$.
- General LWE $q, n, \sigma = \sqrt{\frac{n}{2 \cdot \pi}}$

$$\mathcal{O}\left(n \cdot 2^{\omega \cdot \mathcal{O}\left(n^{1.2787}\right)}\right), \quad p_{success} \geq 1 - \frac{2}{\pi \cdot \sqrt{n}}.$$

- Small error LWE $|\mathcal{E}| = D$

$$\mathcal{O}\left(m \cdot (D-1) \cdot n \cdot 2^{\omega \cdot \mathcal{O}(n)}\right).$$

- Small secret LWE $|\mathcal{S}| = D$

$$\mathcal{O}\left(m \cdot (D-1) \cdot n^2 \cdot 2^{\omega \cdot \mathcal{O}\left(n^{1.2787}\right)}\right).$$

- Previous analysis [ACF+15] assumed that $\mathcal{F}_{\text{LWE}}$ is semi-regular.
  - $d_{\text{reg}}\left(\mathcal{F}_{\text{LWE}}\right)$ computable.
  - $d_{\text{reg}}\left(\mathcal{F}_{\text{LWE}}\right)$ DRL Gröbner basis complexity measure.

Degree of Regularity as Complexity Measure

- Previous analysis [ACF+15] assumed that $\mathcal{F}_{\text{LWE}}$ is semi-regular.
  - $d_{\text{reg}}\left(\mathcal{F}_{\text{LWE}}\right)$ computable.
  - $d_{\text{reg}}\left(\mathcal{F}_{\text{LWE}}\right)$ DRL Gröbner basis complexity measure.

Refined DRL Solving Degree [CG23, Definition 1.1]

- $\mathcal{F} \subset P = K[x_1, \ldots, x_n]$, $d \in \mathbb{Z}$.

Degree of Regularity as Complexity Measure

- Previous analysis [ACF+15] assumed that $\mathcal{F}_{\text{LWE}}$ is semi-regular.
  - $d_{\text{reg}}\left(\mathcal{F}_{\text{LWE}}\right)$ computable.
  - $d_{\text{reg}}\left(\mathcal{F}_{\text{LWE}}\right)$ DRL Gröbner basis complexity measure.

Refined DRL Solving Degree [CG23, Definition 1.1]

- $\mathcal{F} \subset P = K[x_1, \ldots, x_n]$, $d \in \mathbb{Z}$.
- $\boldsymbol{M}_{\leq d}\left(\mathcal{F}\right)$ Macaulay matrix for $\mathcal{F}$, $\mathcal{B}_1 = \text{rowsp}\left(\boldsymbol{M}_{\leq d}\left(\mathcal{F}\right)\right)$.

UNIVERSITÄT KLAGENFURT

erc European Research Council

Degree of Regularity as Complexity Measure

- Previous analysis [ACF+15] assumed that $\mathcal{F}_{\text{LWE}}$ is semi-regular.
  - $d_{\text{reg}}\left(\mathcal{F}_{\text{LWE}}\right)$ computable.
  - $d_{\text{reg}}\left(\mathcal{F}_{\text{LWE}}\right)$ DRL Gröbner basis complexity measure.

Refined DRL Solving Degree [CG23, Definition 1.1]

- $\mathcal{F} \subset P = K[x_1, \dots, x_n]$, $d \in \mathbb{Z}$.
- $\boldsymbol{M}_{\leq d}\left(\mathcal{F}\right)$ Macaulay matrix for $\mathcal{F}$, $\mathcal{B}_1 = \text{rowsp}\left(\boldsymbol{M}_{\leq d}\left(\mathcal{F}\right)\right)$.
- $\boldsymbol{M}_{\leq d}\left(\mathcal{B}_1\right)$ Macaulay matrix for $\mathcal{B}_1$, $\mathcal{B}_2 = \text{rowsp}\left(\boldsymbol{M}_{\leq d}\left(\mathcal{B}_1\right)\right)$.

Degree of Regularity as Complexity Measure

- Previous analysis [ACF$^+$15] assumed that $\mathcal{F}_{\text{LWE}}$ is semi-regular.
  - $d_{\text{reg}}\left(\mathcal{F}_{\text{LWE}}\right)$ computable.
  - $d_{\text{reg}}\left(\mathcal{F}_{\text{LWE}}\right)$ DRL Gröbner basis complexity measure.

Refined DRL Solving Degree [CG23, Definition 1.1]

- $\mathcal{F} \subset P = K[x_1, \ldots, x_n]$, $d \in \mathbb{Z}$.
- $\boldsymbol{M}_{\leq d}\left(\mathcal{F}\right)$ Macaulay matrix for $\mathcal{F}$, $\mathcal{B}_1 = \text{rowsp}\left(\boldsymbol{M}_{\leq d}\left(\mathcal{F}\right)\right)$.
- $\boldsymbol{M}_{\leq d}\left(\mathcal{B}_1\right)$ Macaulay matrix for $\mathcal{B}_1$, $\mathcal{B}_2 = \text{rowsp}\left(\boldsymbol{M}_{\leq d}\left(\mathcal{B}_1\right)\right)$.
- Iterate until $\mathcal{B}_i = \mathcal{B}_{i+1}$.

Degree of Regularity as Complexity Measure

- Previous analysis [ACF+15] assumed that $\mathcal{F}_{\text{LWE}}$ is semi-regular.
  - $d_{\text{reg}}\left(\mathcal{F}_{\text{LWE}}\right)$ computable.
  - $d_{\text{reg}}\left(\mathcal{F}_{\text{LWE}}\right)$ DRL Gröbner basis complexity measure.

Refined DRL Solving Degree [CG23, Definition 1.1]

- $\mathcal{F} \subset P = K[x_1, \dots, x_n]$, $d \in \mathbb{Z}$.
- $\boldsymbol{M}_{\leq d}\left(\mathcal{F}\right)$ Macaulay matrix for $\mathcal{F}$, $\mathcal{B}_1 = \text{rowsp}\left(\boldsymbol{M}_{\leq d}\left(\mathcal{F}\right)\right)$.
- $\boldsymbol{M}_{\leq d}\left(\mathcal{B}_1\right)$ Macaulay matrix for $\mathcal{B}_1$, $\mathcal{B}_2 = \text{rowsp}\left(\boldsymbol{M}_{\leq d}\left(\mathcal{B}_1\right)\right)$.
- Iterate until $\mathcal{B}_i = \mathcal{B}_{i+1}$.
- $\overline{\text{sd}}_{DRL}\left(\mathcal{F}\right)$ least $d \in \mathbb{Z}_{\geq 0}$ such that Gaussian elimination on iterated Macaulay matrices produces DRL-Gröbner basis.

UNIVERSITÄT KLAGENFURT

erc European Research Council

Theorem

- $\mathcal{F} \subset K[x_1, \ldots, x_n]$, $d_{\text{reg}}(\mathcal{F}) < \infty$.
- $\overline{\text{sd}}_{DRL}(\mathcal{F}) \leq 2 \cdot d_{\text{reg}}(\mathcal{F}) - 1$.
- *Complexity*

$$\mathcal{O}\left(m \cdot \overline{\text{sd}}_{DRL}(\mathcal{F})^3 \cdot \binom{n + \overline{\text{sd}}_{DRL}(\mathcal{F}) - 1}{\overline{\text{sd}}_{DRL}(\mathcal{F})}^{\omega + 2} \right).$$

Two Approaches To LWE Complexity Estimation

Gaussian elimination on

- Iterated Macaulay matrices.
- $\overline{\text{sd}}_{DRL}(\mathcal{F}) \leq 2 \cdot d_{\text{reg}}(\mathcal{F}) - 1$.
- Complexity:

$$\mathcal{O}\left(\binom{n + \overline{\text{sd}}_{DRL}(\mathcal{F}) - 1}{\overline{\text{sd}}_{DRL}(\mathcal{F})}^{\omega+2}\right).$$

UNIVERSITÄT KLAGENFURT

erc European Research Council

Two Approaches To LWE Complexity Estimation

Gaussian elimination on

- Iterated Macaulay matrices.
- $\overline{\text{sd}}_{DRL}\left(\mathcal{F}\right) \leq 2 \cdot d_{\text{reg}}\left(\mathcal{F}\right) - 1$.
- Complexity:

$$\mathcal{O}\left(\binom{n + \overline{\text{sd}}_{DRL}\left(\mathcal{F}\right) - 1}{\overline{\text{sd}}_{DRL}\left(\mathcal{F}\right)}^{\omega+2}\right).$$

- Single Macaulay matrix.
- $\text{sd}_{DRL}\left(\mathcal{F}\right) \leq \text{reg}\left(\mathcal{F}^{\text{hom}}\right)$.
- $d_{\text{reg}}\left(\mathcal{F}\right) \leq \text{reg}\left(\mathcal{F}^{\text{hom}}\right)$ [CG23, Theorem 5.3].
- Complexity:

$$\mathcal{O}\left(\binom{n + \text{sd}_{DRL}\left(\mathcal{F}\right) - 1}{\text{sd}_{DRL}\left(\mathcal{F}\right)}^{\omega}\right).$$

UNIVERSITÄT KLAGENFURT

erc European Research Council

How To Compute Degree of Regularity?

$\mathcal{F}_{\text{LWE}} = \{f_1, \dots, f_m\} \subset P = \mathbb{F}_q[x_1, \dots, x_n]$, $\forall i : \deg(f_i) = D$

- Compute DRL Gröbner basis of homogeneous system

$$\left(\mathcal{F}_{\text{LWE}}^{\text{top}}\right) = \left(\mathcal{F}_{\text{LWE}}^{\text{hom}}, x_0\right).$$

How To Compute Degree of Regularity?

$\mathcal{F}_{\text{LWE}} = \{f_1, \dots, f_m\} \subset P = \mathbb{F}_q[x_1, \dots, x_n]$, $\forall i \colon \deg(f_i) = D$

- Compute DRL Gröbner basis of homogeneous system

$$\left(\mathcal{F}_{\text{LWE}}^{\text{top}}\right) = \left(\mathcal{F}_{\text{LWE}}^{\text{hom}}, x_0\right).$$

  - Infeasible in practice.

How To Compute Degree of Regularity?

$\mathcal{F}_{\text{LWE}} = \{f_1, \ldots, f_m\} \subset P = \mathbb{F}_q[x_1, \ldots, x_n]$, $\forall i : \deg(f_i) = D$

- Compute DRL Gröbner basis of homogeneous system

$$\left(\mathcal{F}_{\text{LWE}}^{\text{top}}\right) = \left(\mathcal{F}_{\text{LWE}}^{\text{hom}}, x_0\right).$$

  - Infeasible in practice.

- But we can estimate **"Lowest Achievable Degree of Regularity"** via necessary condition:

$$|\mathcal{F}_{\text{LWE}}| \cdot \underbrace{\binom{n+d-1}{d}}_{=\dim_{\mathbb{F}_q}(P_d)} \overset{!}{\geq} \underbrace{\binom{n+D+d-1}{D+d-1}}_{=\dim_{\mathbb{F}_q}(P_{D+d})}.$$

UNIVERSITÄT KLAGENFURT

erc European Research Council

LWE Worst Case Complexity estimation

- Specify LWE parameters q, n, m, χ, and LWE polynomial degree D.

LWE Worst Case Complexity estimation

- Specify LWE parameters q, n, m, χ, and LWE polynomial degree D.
- Evaluate $m \cdot \binom{n+d-1}{d} \overset{!}{\geq} \binom{n+D+d-1}{D+d-1}$ to find estimator $\hat{d}_{\text{reg}} = D + d$.

UNIVERSITÄT KLAGENFURT

erc European Research Council

LWE Worst Case Complexity estimation

- Specify LWE parameters q, n, m, χ, and LWE polynomial degree D.
- Evaluate $m \cdot \binom{n+d-1}{d} \overset{!}{\geq} \binom{n+D+d-1}{D+d-1}$ to find estimator $\hat{d}_{\text{reg}} = D + d$.
- Evaluate $\mathcal{O}\left(\binom{n+\hat{d}_{\text{reg}}-1}{\hat{d}_{\text{reg}}}^{\omega}\right)$ for security level.

UNIVERSITÄT KLAGENFURT

erc European Research Council

LWE Worst Case Complexity estimation

- Specify LWE parameters q, n, m, χ, and LWE polynomial degree D.
- Evaluate $m \cdot \binom{n+d-1}{d} \overset{!}{\geq} \binom{n+D+d-1}{D+d-1}$ to find estimator $\hat{d}_{\text{reg}} = D + d$.
- Evaluate $\mathcal{O}\left(\binom{n+\hat{d}_{\text{reg}}-1}{\hat{d}_{\text{reg}}}^{\omega}\right)$ for security level.

UNIVERSITÄT KLAGENFURT

erc European Research Council

LWE Worst Case Complexity estimation

- Specify LWE parameters q, n, m, χ, and LWE polynomial degree D.
- Evaluate $m \cdot \binom{n+d-1}{d} \overset{!}{\geq} \binom{n+D+d-1}{D+d-1}$ to find estimator $\hat{d}_{\text{reg}} = D + d$.
- Evaluate $\mathcal{O}\left(\binom{n+\hat{d}_{\text{reg}}-1}{\hat{d}_{\text{reg}}}^{\omega}\right)$ for security level.

Binary Secret LWE

- n, m, $\mathcal{F}_{\text{LWE}} = \{f_1, \ldots, f_m, x_1^2 - x_1, \ldots, x_n^2 - x_n\}$, $D = \deg(f_i)$.

LWE Worst Case Complexity estimation

- Specify LWE parameters q, n, m, χ, and LWE polynomial degree D.
- Evaluate $m \cdot \binom{n+d-1}{d} \overset{!}{\geq} \binom{n+D+d-1}{D+d-1}$ to find estimator $\hat{d}_{\text{reg}} = D + d$.
- Evaluate $\mathcal{O}\left(\binom{n+\hat{d}_{\text{reg}}-1}{\hat{d}_{\text{reg}}}^{\omega}\right)$ for security level.

Binary Secret LWE

- n, m, $\mathcal{F}_{\text{LWE}} = \{f_1, \ldots, f_m, x_1^2 - x_1, \ldots, x_n^2 - x_n\}$, $D = \deg(f_i)$.
- Necessary condition simplifies to: $m \cdot \binom{n}{d} \overset{!}{\geq} \binom{n}{D+d}$.

UNIVERSITÄT KLAGENFURT

erc European Research Council

LWE Worst Case Complexity estimation

- Specify LWE parameters q, n, m, χ, and LWE polynomial degree D.
- Evaluate $m \cdot \binom{n+d-1}{d} \overset{!}{\geq} \binom{n+D+d-1}{D+d-1}$ to find estimator $\hat{d}_{\text{reg}} = D + d$.
- Evaluate $\mathcal{O}\left(\binom{n+\hat{d}_{\text{reg}}-1}{\hat{d}_{\text{reg}}}^{\omega}\right)$ for security level.

Binary Secret LWE

- n, m, $\mathcal{F}_{\text{LWE}} = \{f_1, \ldots, f_m, x_1^2 - x_1, \ldots, x_n^2 - x_n\}$, $D = \deg(f_i)$.
- Necessary condition simplifies to: $m \cdot \binom{n}{d} \overset{!}{\geq} \binom{n}{D+d}$.
- If $m \in \mathcal{O}(n^D)$, then complexity $\mathcal{O}\left(n^D \cdot D \cdot 2^{\omega \cdot \mathcal{O}\left(n^{0.6393}\right)}\right)$.

UNIVERSITÄT KLAGENFURT

erc European Research Council

- Complexity estimation for Kyber768 [SAB+22] with $\omega = 2$.
  - Small secret small error LWE instance with $|\mathcal{S}| = |\mathcal{E}| = 5$.
  - $n = m = 3 \cdot 256$.
  - Complexities of lattice-based attacks are computed via the lattice estimator [APS15].

Method	BKW	USVP	BDD	BDD Hybrid	BDD MiTM Hybrid	Dual	Dual Hybrid	Proven complexity estimate		Iterated Macaulay Matrices		Single Macaulay Matrix	
Samples	2^{226}	768	768	768	768	768	768	768	768^4	768	768^4	768	768^4
Complexity (bits)	239	205	201	201	357	214	206	5554	5581	4717	419	1588	203

LWE With Hints

- Hardness of LWE in presence of side-information.
  - Improvement of lattice attacks [DDGR20, DGHK23].

Types of Hints

- Perfect hints: $\langle \boldsymbol{s}, \boldsymbol{v} \rangle = l \in \mathbb{F}_q$.
- Modular hints: $\langle \boldsymbol{s}, \boldsymbol{v} \rangle \equiv l \mod k$.
- Approximate hints: $\langle \boldsymbol{s}, \boldsymbol{v} \rangle + e_\sigma = l \in \mathbb{F}_q$.
- Short vector hints: $\boldsymbol{v} \in \Lambda_{\text{LWE}}$.

LWE With Hints

- Hardness of LWE in presence of side-information.
  - Improvement of lattice attacks [DDGR20, DGHK23].

Types of Hints

- Perfect hints: $\langle \boldsymbol{s}, \boldsymbol{v} \rangle = l \in \mathbb{F}_q$.
- Modular hints: $\langle \boldsymbol{s}, \boldsymbol{v} \rangle \equiv l \mod k$.
- Approximate hints: $\langle \boldsymbol{s}, \boldsymbol{v} \rangle + e_\sigma = l \in \mathbb{F}_q$.
- Short vector hints: $\boldsymbol{v} \in \Lambda_{\mathsf{LWE}}$.

- In principle any hint which can be modeled in $\mathbb{F}_q[\boldsymbol{x}]$ can be added to $\mathcal{F}_{\mathsf{LWE}}$.

UNIVERSITÄT KLAGENFURT

erc European Research Council

LWE With Hints

- Hardness of LWE in presence of side-information.
  - Improvement of lattice attacks [DDGR20, DGHK23].

Types of Hints

- Perfect hints: $\langle \boldsymbol{s}, \boldsymbol{v} \rangle = l \in \mathbb{F}_q$.
- Modular hints: $\langle \boldsymbol{s}, \boldsymbol{v} \rangle \equiv l \mod k$.
- Approximate hints: $\langle \boldsymbol{s}, \boldsymbol{v} \rangle + e_\sigma = l \in \mathbb{F}_q$.
- Short vector hints: $\boldsymbol{v} \in \Lambda_{\mathsf{LWE}}$.

- In principle any hint which can be modeled in $\mathbb{F}_q[\boldsymbol{x}]$ can be added to $\mathcal{F}_{\mathsf{LWE}}$.
- The closer one can get to binary secret/error LWE the better:

$$m \cdot \binom{n+d-1}{d} \overset{!}{\geq} \binom{n+D+d-1}{D+d} \text{ vs. } m \cdot \binom{n}{d} \overset{!}{\geq} \binom{n}{D+d}.$$

Finite Degree of Regularity for LWE

$$f(x) = x \cdot \prod_{i=1}^{N} (x - i) \cdot (x + i),$$
$$\mathcal{F}_{\text{LWE}} = \left\{ f\left(b_i - \langle \boldsymbol{x}, \boldsymbol{a}_i \rangle \right) \right\}_{1 \leq i \leq m} \subset \mathbb{F}_q[\boldsymbol{x}]$$

- Then
$$\mathcal{F}_{\text{LWE}}^{\text{top}} = \left\{ \left(\langle \boldsymbol{x}, \boldsymbol{a}_i \rangle \right)^{2 \cdot N + 1} \right\}_{1 \leq i \leq m}.$$

$$f(x) = x \cdot \prod_{i=1}^{N} (x - i) \cdot (x + i),$$
$$\mathcal{F}_{\text{LWE}} = \left\{ f\left(b_i - \langle \boldsymbol{x}, \boldsymbol{a}_i \rangle\right) \right\}_{1 \leq i \leq m} \subset \mathbb{F}_q[\boldsymbol{x}]$$

- Then
$$\mathcal{F}_{\text{LWE}}^{\text{top}} = \left\{ \left(\langle \boldsymbol{x}, \boldsymbol{a}_i \rangle \right)^{2 \cdot N + 1} \right\}_{1 \leq i \leq m}.$$
- If $\boldsymbol{A} = \begin{pmatrix} \boldsymbol{a}_1 & \dots & \boldsymbol{a}_m \end{pmatrix}^\intercal$ has rank n, then perform change of coordinates
$$\boldsymbol{y} = \hat{\boldsymbol{A}} \boldsymbol{x}.$$

UNIVERSITÄT KLAGENFURT

erc European Research Council

Finite Degree of Regularity for LWE

$f(x) = x \cdot \prod_{i=1}^{N} (x - i) \cdot (x + i)$,
$\mathcal{F}_{\text{LWE}} = \left\{ f\left(b_i - \langle \boldsymbol{x}, \boldsymbol{a}_i \rangle\right) \right\}_{1 \leq i \leq m} \subset \mathbb{F}_q[\boldsymbol{x}]$

- Then

$$\mathcal{F}_{\text{LWE}}^{\text{top}} = \left\{ \left(\langle \boldsymbol{x}, \boldsymbol{a}_i \rangle \right)^{2 \cdot N + 1} \right\}_{1 \leq i \leq m}.$$

- If $\boldsymbol{A} = \begin{pmatrix} \boldsymbol{a}_1 & \dots & \boldsymbol{a}_m \end{pmatrix}^\intercal$ has rank n, then perform change of coordinates

$$\boldsymbol{y} = \hat{\boldsymbol{A}} \boldsymbol{x}.$$

- Then

$$\left\{ y_1^{2 \cdot N + 1}, \dots, y_n^{2 \cdot N + 1} \right\} \subset \mathcal{F}_{\text{LWE}}^{\text{top}} \quad \Rightarrow \quad d_{\text{reg}}\left(\mathcal{F}_{\text{LWE}} \right) < \infty.$$

Hints Complexity Example

- Impact of hints on small secret small error LWE:
  $|\mathcal{S}| = |\mathcal{E}| = D = 5,\ n = 256,\ m = 256^{\frac{3}{2}}$.

Hints Complexity Example

- Impact of hints on small secret small error LWE: $|\mathcal{S}| = |\mathcal{E}| = D = 5,\ n = 256,\ m = 256^{\frac{3}{2}}$.
- The closer one can move a LWE to binary secret/error LWE the better.
  - Necessary degree of regularity condition: $m \cdot \binom{n+d-1}{d} \overset{!}{\geq} \binom{n+D+d-1}{D+d}$ vs. $m \cdot \binom{n}{d} \overset{!}{\geq} \binom{n}{D+d}$.

Hints Complexity Example

- Impact of hints on small secret small error LWE: $|\mathcal{S}| = |\mathcal{E}| = D = 5,\ n = 256,\ m = 256^{\frac{3}{2}}$.
- The closer one can move a LWE to binary secret/error LWE the better.
  - Necessary degree of regularity condition: $m \cdot \binom{n+d-1}{d} \overset{!}{\geq} \binom{n+D+d-1}{D+d}$ vs. $m \cdot \binom{n}{d} \overset{!}{\geq} \binom{n}{D+d}$.
- Column d lists degree for the lowest achievable degree of regularity $\hat{d}_{\text{reg}}\left(\mathcal{F}_{\text{LWE}}\right) = D + d$.

	Small Secret Small Error LWE $D=5$		Binary Secret LWE $D=5$		Binary Secret Binary Error LWE $D=2$	
Perfect hints	d	Single Macaulay Matrix (bits)	d	Single Macaulay Matrix (bits)	d	Single Macaulay Matrix (bits)
$\omega = 2$						
0	57	481	38	370	3	92
50	45	393	30	303	2	78
150	22	221	15	174	1	59

- Martin R. Albrecht, Carlos Cid, Jean-Charles Faugère, Robert Fitzpatrick, and Ludovic Perret.
  Algebraic algorithms for LWE problems.
  ACM Commun. Comput. Algebra, 49(2):62, aug 2015.
  doi:10.1145/2815111.2815158.

- Sanjeev Arora and Rong Ge.
  New algorithms for learning in presence of errors.
  In Luca Aceto, Monika Henzinger, and Jiri Sgall, editors, *ICALP 2011: 38th International Colloquium on Automata, Languages and Programming, Part I*, volume 6755 of *Lecture Notes in Computer Science*, pages 403–415, Zurich, Switzerland, July 4–8, 2011. Springer, Heidelberg, Germany.
  doi:10.1007/978-3-642-22006-7_34.

Martin R. Albrecht, Rachel Player, and Sam Scott.
On the concrete hardness of Learning with Errors.
J. Math. Cryptol., 9(3):169–203, 2015.
doi:10.1515/jmc-2015-0016.

Magali Bardet, Jean-Charles Faugère, and Bruno Salvy.
On the complexity of Gröbner basis computation of semi-regular overdetermined algebraic equations.
In *Proceedings of the International Conference on Polynomial System Solving*, pages 71–74, 2004.

Bruno Buchberger.
Ein Algorithmus zum Auffinden der Basiselemente des Restklassenringes nach einem nulldimensionalen Polynomideal.
PhD thesis, Universität Innsbruck, 1965.

References III

Alessio Caminata and Elisa Gorla.
Solving multivariate polynomial systems and an invariant from commutative algebra.
In Jean Claude Bajard and Alev Topuzoğlu, editors, *Arithmetic of Finite Fields*, pages 3–36, Cham, 2021. Springer International Publishing.
doi:10.1007/978-3-030-68869-1_1.

Alessio Caminata and Elisa Gorla.
Solving degree, last fall degree, and related invariants.
J. Symb. Comput., 114:322–335, 2023.
doi:10.1016/j.jsc.2022.05.001.

References IV

Dana Dachman-Soled, Léo Ducas, Huijing Gong, and Mélissa Rossi.
LWE with side information: Attacks and concrete security estimation.
In Daniele Micciancio and Thomas Ristenpart, editors, *Advances in Cryptology – CRYPTO 2020, Part II*, volume 12171 of *Lecture Notes in Computer Science*, pages 329–358, Santa Barbara, CA, USA, August 17–21, 2020. Springer, Heidelberg, Germany.
doi:10.1007/978-3-030-56880-1_12.

References V

Dana Dachman-Soled, Huijing Gong, Tom Hanson, and Hunter Kippen.
Revisiting security estimation for LWE with hints from a geometric perspective.
In Helena Handschuh and Anna Lysyanskaya, editors, *Advances in Cryptology – CRYPTO 2023, Part V*, volume 14085 of *Lecture Notes in Computer Science*, pages 748–781, Santa Barbara, CA, USA, August 20–24, 2023. Springer, Heidelberg, Germany.
doi:10.1007/978-3-031-38554-4_24.

Peter Schwabe, Roberto Avanzi, Joppe Bos, Léo Ducas, Eike Kiltz, Tancrède Lepoint, Vadim Lyubashevsky, John M. Schanck, Gregor Seiler, Damien Stehlé, and Jintai Ding.
CRYSTALS-KYBER.
Technical report, National Institute of Standards and Technology, 2022.
available at https://csrc.nist.gov/Projects/post-quantum-cryptography/selected-algorithms-2022.

Chao Sun, Mehdi Tibouchi, and Masayuki Abe.
Revisiting the hardness of binary error LWE.
In Joseph K. Liu and Hui Cui, editors, *ACISP 20: 25th Australasian Conference on Information Security and Privacy*, volume 12248 of *Lecture Notes in Computer Science*, pages 425–444, Perth, WA, Australia, November 30 – December 2, 2020. Springer, Heidelberg, Germany.
doi:10.1007/978-3-030-55304-3_22.

Matthias Johann Steiner.
Solving degree bounds for iterated polynomial systems.
IACR Transactions on Symmetric Cryptology, 2024(1):357–411, 2024.
doi:10.46586/tosc.v2024.i1.357-411.

Arne Storjohann.
Algorithms for matrix canonical forms.
Doctoral thesis, ETH Zurich, Zürich, 2000.
Diss., Technische Wissenschaften ETH Zürich, Nr. 13922, 2001.
doi:10.3929/ethz-a-004141007.